

USER MANUAL

VRM-308

8-VDSL + 2-Giga Ethernet Managed 4-Band VDSL IP DSLAM



The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.

HyperTerminal™ is a registered trademark of Hilgraeve Inc.

WARNING:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR PUB.22 Class A COMPLIANCE:

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

WARNING:

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CE NOTICE

Marking by the symbol CE indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:1994/A1:1995/A2:1997 Class A and EN61000-3-2:1995, EN61000-3-3:1995 and EN50082-1:1997

CTC Union Technologies Co., Ltd.

Far Eastern Vienna Technology Center (Neihu Technology Park)

8F, No. 60, Zhouzi St.

Neihu, Taipei, 114

Taiwan

Phone: +886-2-2659-1021

FAX: +886-2-2799-1355

VRM-308

8-VDSL+2-Giga Ethernet Managed 4-Band VDSL IP DSLAM

User Manual

Version 1.0 Jun. 2007 First Release

This manual supports the following models:

VRM-308 AC

This document is the first official release manual. Please check CTC Union's website for any updated manual or contact us by E-mail at info@ctcu.com. Please address any comments for improving this manual or to point out omissions or errors to marketing@ctcu.com. Thank you.

Table of Contents

1. Introduction	7
1.1 VDSL Solution.....	7
1.2 Unpacking Information	8
1.3 Product Details.....	8
1.4 Description.....	10
2. Installation	11
2.1 Hardware Installation Introduction	11
2.2 Pre-Installation Requirements	11
2.3 General Rules.....	11
2.4 Connecting the IP DSLAM.....	11
3. Management Configuration	13
3.1 Local Management	13
3.2 Remote Network Management	15
3.2.2.1. Web Management Home Overview	16
3.2.2.2. Port status	16
3.2.2.3. Port Statistics.....	17
3.2.2.4. Administrator.....	17
3.2.2.5. IP Address	18
3.2.2.6. Switch Settings.....	18
3.2.2.7. Console Port Information	20
3.2.2.8. Port Controls, VDSL Speed Control and port Enable/Disable	20
3.2.2.9. Link Aggregation	21
3.2.2.10. Filter Database	23
3.2.2.11. VLAN configuration.....	25
3.2.2.12. Spanning Tree.....	27
3.2.2.13. Port Mirroring	28
3.2.2.14. SNMP	29
3.2.2.15. SNR.....	30
3.2.2.16. Security Manager	30
3.2.2.17. TFTP Update Firmware	31
3.2.2.18. Configuration Backup/Restore.....	31
3.2.2.19. Reset System	31
3.2.2.20. Reboot.....	31
4. Applications.....	33
Appendix A: Troubleshooting	35
Diagnosing VDSL Indicators	35
System Diagnostics.....	35
Appendix B: VDSL Spectrum	37
Appendix C: Example of VLAN Setting.....	38

Table of Contents

1. Introduction

1.1 VDSL Solution

The 4-Band VDSL IP DSLAM networking solution delivers cost-effective, high-performance broadband access to multi-unit buildings (hotels, apartment, and multi-tenant office buildings) and enterprise environments such as manufacturing, educational campuses, and medical facilities. VDSL technology dramatically extends Ethernet over existing Category 1/2/3 wiring at speeds from 5/15/25 Mbps (full duplex) and distances up to 600/1100/1700 meters. VDSL technology delivers broadband service on the same lines as Plain Old Telephone Service (POTS), digital telephone, and ISDN systems. In addition, VDSL supports modes compatible with symmetric digital subscriber line, allowing service providers to provision VDSL to buildings where broadband services already exist.

The 4-Band VDSL solution includes an 8 port IP DSLAM (CO side) and 4-Band VDSL stand-alone modems as CPE devices. The 4-Band VDSL solution delivers everything needed to quickly deploy an Ethernet-based network with the performance required to deliver high-speed Internet access at much greater distances than Ethernet and to drive services like IP telephony and audio/video streaming. With this technology, a broad range of customers can benefit from lower operating costs and rapid deployment. The 4-Band VDSL solution provides multicast, Layer 2 quality of service (QoS), Link Aggregation (LACP) dynamic trunking group, security, GVRP, IGMP for VOD (Video on demand) and SNMP RMON management with Web-based Switch management.

The 4-Band VDSL IP DSLAM is a bridge between external Internet backbone through a router for IP sharing and the building's 110D telephone rack or telephone box. It utilizes the available telephone wire to enable high-speed Internet access to building residents. The 4-Band IP DSLAM utilizes the already existing telephone wire to deliver 5/15/25 Mbps Internet access on each RJ-45 port. This gives users a lower-cost, end-to-end solution and eliminates the expense of installing new or additional UTP cabling.

8 Ports 5/15/25M 4-Band VDSL IP DSLAM + 2 10/100/1000M Giga Ethernet

The 4-Band IP DSLAM has 8 x 5/15/25M VDSL ports and 2 x 10/100/1000M Ethernet ports. The IP DSLAM is a one unit tall rack (1RU) by 10-inches deep. It is a standard Rack mounted size. 4-Band IP DSLAM delivers dedicated bandwidth per port at rates of 5/15/25 Mbps. VDSL transmissions co-exist with POTS or ISDN, and can be compatible with ADSL/HomePNA traffic in the same building. The switches can be configured on a per-switch port basis to support the following modes:

- **5 Mbps symmetrical rate (up to 1700 meters)**
- **15 Mbps symmetrical rate (up to 1100 meters)**
- **25 Mbps symmetrical rate (up to 600 meters)**

The 4-Band VDSL IP DSLAM with 4-Band VDSL Modems provide fast and easy connectivity into building patch panels with RJ-45 connector. The 10/100/1000 Giga Ethernet ports can be used to connect servers or Ethernet switches. These connectivity options provide multiple price/performance options to meet building and budget requirements. The 4-Band IP DSLAM provides these important features necessary for robust networks.

- **Class of Service:** 802.1p QoS support. Provides high and low priority queuing on a per-port basis.
- **Supports:** IGMP Snooping with 512 IP multicast table for VOD (Video on demand) and video conference and internet games application.
- **Scalability:** Up to 5/15/25 Mbps symmetric performance over single-pair wiring. Fast Ethernet Channel port aggregation.
- **Security:** 802.1Q Tag-based and 802.1V protocol-based virtual local-area network (VLAN) support. Private VLAN access, assures port security without requiring a VLAN per port, and also supports MAC filtering.
- **Local Management :** IP DSLAM provides a serial console port for setting IP or other functions.
- **Remote Management:** IP DSLAM supports remote configuration and monitoring by Telnet and Web-based GUI. This software is embedded in the VDSL SWITCH and delivers remote, intuitive management of the IP DSLAM and connected VDSL CPE devices through a single IP address.
- **IEEE-802.1d STP:** Spanning Tree Protocol is a bridging protocol to avoid port looping and for link redundancy.

- **IEEE-802.1ad Link Aggregation:** This protocol allows port trunking or bundling for increased bandwidth.
- **Port Mirroring:** This function is used by a network administrator to allow traffic monitoring with sniffer software or network analyzer.
- **Broadcast storm filtering:** This function can avoid connecting a node that has excessive broadcast packets.
- **TFTP protocol:** This function is used for remote firmware upgrade and setup value backup and restore.
- **SNMP:** Support RFC-1493 bridge MIB; RFC-1213 MIB II; RFC-1643 Ethernet MIB and RFC-1757 RMON MIB with 1,2,3,9 groups
- **SNR (Signal to Noise Ratio) indication :** This function checks CO and CPE connection quality over phone wiring.
- **Alarm :** Through WEB or Telnet, you can show internal temperature and fan speed. If temperature exceeds 70°C or fan stops, the Switch will send an SNMP trap to inform the Trap management server.
- **Cracker prevention:** To avoid intruders from entering the management system through the client side, the 8 port IP DSLAM will filter system IP from client side, preventing attack.
- **Supports for multiple web browsers:** IE, Mozilla (Firefox) & Netscape under Windows O/S or Mozilla & Netscape under Linux and MAC O/S.

1.2 Unpacking Information

Carefully unpack the package and check its contents against the checklist.

Check List

1. 4-Band VDSL IP DSLAM, 2 x10/100/1000 Giga Ethernet ports and 8 x 5/15/25Mbps VDSL ports
2. 1 x Users manual CD
3. 1 x AC Power Cord
4. 2 x Rack Mounting Brackets
5. 4 x Screws
6. 4 x Plastic feet

Please inform your dealer or shipper immediately if anything is missing or damaged. If possible, retain the original carton, including the original packing materials. Use them to repack the unit in case there is a need to return for repair.

1.3 Product Details



Product Name: 2 ports 10/100/1000Mbps Gigabit Ethernet plus 8 ports 4-Band VDSL IP DSLAM with SNMP

- Application : hotel/campus/hospital/factory/Telecom

Features

- Supports 5M/15M/25Mbps per port symmetrical bandwidth over phone wiring with long drive capability 1.7/1.1/0.6Km(5666/3666/1999 feet) with auto-negotiated speed.
- Provides 2 x 10/100/1000Mbps Ethernet RJ-45 Ports with Auto MDI/MDIX
- Supports quality of phone wiring detected with SNR(Signal to Noise Ratio) indications
- Supports GARP/GVRP IEEE-802.1p/q VLAN with 256 groups static VID or 4094 groups dynamic VID
- Supports port base V-Lan
- Supports IEEE 802.1v protocol V-Lan
- Supports QoS IEEE-802.1p
- Supports Multicast IP table/IGMP v2 with 512 groups
- Supports LACP IEEE-802.1ad Port Trunking (Link aggregation)
- Supports IEEE 802.1d Spanning Tree Protocol for MAC bridge with redundant link
- Supports port Mirroring (Sniffer)
- Supports Broadcast Storm filtering

- Ethernet transport with POTS / ISDN traffic over single copper wire pair
- Spectral compatibility with xDSL, ISDN(2B1Q/4B3T), HomePNA
- Supports port security with MAC address filtering & IP limitation.
- Supports Web Based and Telnet remote management
- Supports system POST LED
- Supports SNMP v1 RFC-1493 Bridge MIBs
RFC-1643 Ethernet MIB
RFC-1213 MIB II
Enterprise MIB (Fan and Temperature management)
Supports RMON groups 1(Statistics), 2(Alarm), 3(Event), 9(History)
- Cascades up to 8 Units along with Gigabit switch
- Supports TFTP/XMODEM firmware upgrade
- Supports In-Band/Out-of-Band Management
- Supports Fan & Temperature Monitor & management
- Surge protection for VDSL ports
- POTS Splitters built-in

Specifications

- Compliant with IEEE 802.3 & 802.3u Ethernet Standards
- Compliant with ETSI, ITU, ANSI standards
- 10/100/1000Mbps Ethernet ports: 2 x RJ-45 with auto MDIX
- POTS/ISDN Splitter ports: 8 x RJ-45
- VDSL port: 8 x RJ-45
- MAC address table: 8K Entries
- Switching method: Store-and-forward
- Flow control method by IEEE802.3x for Full Duplex & Back Pressure for Half Duplex
- Compliant with GARP/GVRP IEEE 802.1p/q port-base VLAN with 256 groups static VID or 4094 dynamic VID
- Compliant with IEEE 802.1v protocol-base VLAN classification
- Compliant with IEEE 802.1d Spanning Tree Protocol
- Multicast IP table: 512 groups
- Compliant with IEEE 802.1p QoS by class of service with 2-level priority queuing
- Compliant with LACP IEEE 802.3ad Link Aggregation
- RS-232 console port: DB-9 Pin Female / 9600bps
- SNMP v1 RFC-1493 Bridge MIBs
RFC-1643 Ethernet MIB
RFC-1213 MIB II
Enterprise MIBs
RMON groups 1(Statistics), 2(Alarms), 3(Events), 9(History)
- Port security by MAC address filtering
- LED indication:
Power good and POST LED
Link/Active/Speed Status for Ethernet ports
Link for VDSL ports
- VDSL Frequency Spectrum:
Transmitter: 0.9 ~ 3.9 MHz
Receiver: 4 ~ 7.9 MHz
- POTS/ISDN pass filter Spectrum: 0 ~ 630 kHz
- Internal switching power supply, Input: AC 100-240 volts/50-60Hz/1A.
- Dimensions: 435 x 255 x 44 mm
- Operating Temperature: 0°C ~ 50°C (32F ~ 122F)
- Storage Temperature: - 20°C ~ 65° C (-4F ~ 149F)
- Humidity: 10%~90% non-condensing
- Certifications: FCC, CE
- RoHS compliant

1.4 Description

Hardware Description

This section describes the important parts of the IP DSLAM. It features the front and rear panel drawings showing the LEDs and connectors.

Front Panel

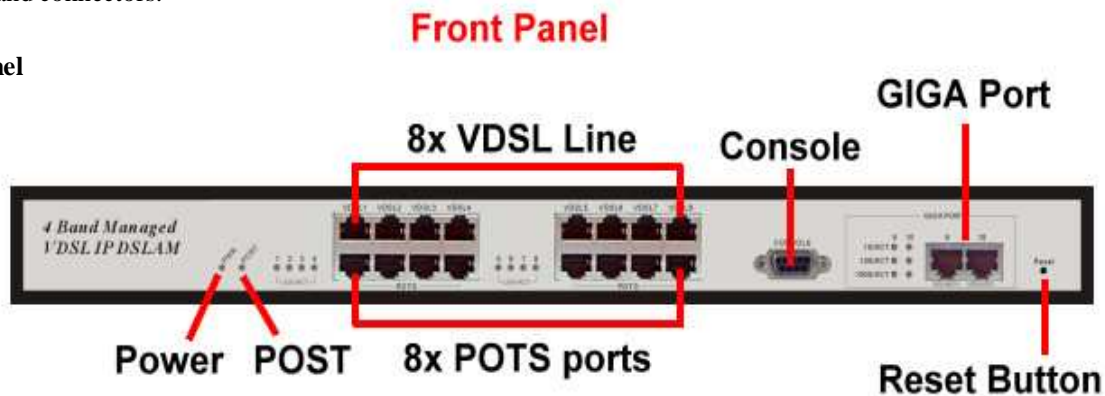


Figure 1.2 Front Panel Description

"PWR": Power LED

"POST": Power On Self Test LED

2 X 10/100/1000 Mbps Gigabit Ethernet ports

8 X 5/15/25 Mbps VDSL Ports.

8 X POTS/ISDN Ports.

RS-232 Console Port

Reset Button (recessed)

The IP DSLAM features built-in POTs Splitters between every VDSL port and POTS(ISDN) side. This allows delivery of VDSL broadband service on the same lines as Plain Old Telephone Service (POTS), PBX, or ISDN traffic. There are several LED indicators for monitoring the device itself, and the network status. At a quick glance of the front panel, the user will be able to tell if the product is receiving power; if it is monitoring another IP DSLAM or IP DSLAMs; or if a problem exists on any port or the network.

LED Indications

The following describes the function of each LED indicator.

LED	State	Functional Description
PWR (Power LED)	Steady Green	This LED light is located on the left side on the front panel. It will light up (ON) to show that the product is receiving power. Conversely, no light (OFF) indicates the product is not receiving input power.
POST	Steady	POST(Power On Self Test) POST Led will light to show system is booting now. When system is ready the LED will be off.
VDSL Link	Steady	Each RJ45 port on the VDSL is assigned an LED light for "Link Good". Each LED is normally OFF after the power on operation, but will light up steadily to show good link.
10 100 1000 LINK/ACT	Steady Green Flashing	Each RJ45 port on the Ethernet is assigned an LED for "10M, 100M and 1000M speed Link". Each LED is normally OFF after the power on operation, but will light up steadily to show good link at speed and flash to show data transmission.

Rear Panel



Figure 3 Rear Panel

AC Power Socket (IEC Type)

The power cord should be plug into this socket. The AC Socket accepts 100 to 240VAC @ 1A.

2. Installation

2.1 Hardware Installation Introduction

This chapter describes how to install the IP DSLAM and to establish a network connection. You may install the IP DSLAM on any level surface (table, shelf, 19 inch rack or wall mounting). However, please note the following minimum site requirements before you begin.

2.2 Pre-Installation Requirements

Before you start actual hardware installation, make sure you can provide the right operating environment, including power requirements, sufficient physical space, and proximity to other network devices that are to be connected. Verify the following installation requirement:

- Power requirements: AC 100V to 240 V at 50 to 60 Hz.
The internal switching power supply automatically adjusts to the input voltage level.
- The IP DSLAM should be located in a cool dry place, with at least 10cm/4in of space at the front and back for ventilation.
- Do not place the IP DSLAM in direct sunlight, near heat sources or in areas with a high amount of electromagnetic interference.
- Check if network cables and connectors needed for installation are available.

2.3 General Rules

Before making any connections to the IP DSLAM, note the following rules:

- Ethernet Port (RJ-45)
All network connections to the IP DSLAM Ethernet port must be made using Category 6 UTP for 1000Mbps, Category 5 UTP for 100Mbps, or Category 3, 4 UTP for 10Mbps.
No more than 100 meters (about 328 feet) of cabling may be use between IP DSLAMs or other network devices.
- VDSL Port (RJ-45)
All phone network connections to the VDSL Port should be made using 18 ~ 26 AWG (American Wire Gauge) phone wiring. We do not recommend using 28 AWG or smaller phone line.

2.4 Connecting the IP DSLAM

The IP DSLAM has 2 10/100/1000 Mbps Gigabit Ethernet ports which support connection to 10/100/1000Mbps Ethernet and support full or half-duplex operation. The transmission mode uses auto-negotiation with fallback to half duplex. Therefore, the devices attached to these ports must support auto-negotiation or they must always operate at half duplex. If transmissions must run at full duplex, but the attached device does not support auto-negotiation, then you should upgrade that device to newer equipment that supports auto-negotiation.

Connecting Station Ports

You may connect the ports "9 & 10" on the IP DSLAM to any device that uses a standard Ethernet interface, such as a Cable modem, ADSL modem, Ethernet Switch, workstation or server, or to a network interconnection device such as a bridge or router (depending on the port type implemented). Prepare the network devices you wish to connect. Make sure you have installed suitable VDSL Modems before making a connection to any of the IP DSLAM (1-8) station ports. You will also need to prepare 18 ~ 26 gauge twisted pair phone line wiring with RJ-45 plugs at both ends. Connect one end of the cable to the RJ-45 port of the VDSL modem network adapter, and the other end to any available (1~8) station port on the VDSL. Each port supports 5/15/25 Mbps connections. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Note:

Do not plug an RJ-11 phone jack connector directly into an Ethernet port (RJ-45 port). This may cause damage to the VDSL. For Ethernet, use only Category 5 twisted-pair cables with RJ-45 connectors that conform to FCC standards. Be sure each twisted-pair cable (UTP) is not over by 100 meters (328 feet). The VDSL RJ-45 ports may use 18 ~ 26 gauge phone wiring. However, 28 gauge or above is not recommended.

This page left blank intentionally.

3. Management Configuration

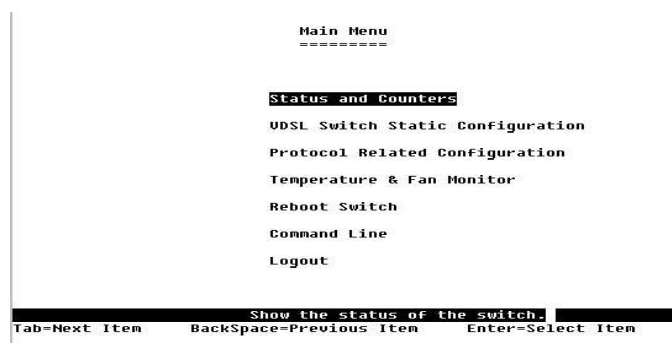
3.1 Local Management

Console port (RS-232) Configuration (Change IP Address By Terminal)

You can configure the device through the local serial console port. Located on the front panel of the device is a DB9 Female connector. Using the supplied serial cable, connect this port to one of the COM ports on a PC or notebook. Boot Windows 95/98/ME/2000/XP system and run the HyperTerminal™ program. Setup the communication parameters as follows.



1. Set "Bits per second" to 9600 via the pull-down menu.
 2. Set "Flow control" to None.
 3. Connect PC COM port to the IP DSLAM. You will be presented with the user login screen.
- Enter
Login name : "admin" ; password : "123"
The Main Menu screen will display after successful login.



4. Operating Keys:

- Tab=Next Item;
- Backspace=Previous Item
- Enter=Select Item
- <Edit>=Enter user keyed-in data
- <Save>=Saves user keyed-in data
- <Quit>=Leave an action menu
- <CTRL-A>=Return to action menu choices

Set IP Address: Please follow these steps

- (1) Select **Switch Static Configuration** with Tab and press Enter

Chapter 3 Management Configuration

(2) On the **Administration Configuration** item, press Enter

```
VDSL Switch :      Switch Configuration
=====

Administration Configuration
Port/Trunk Configuration
Port Mirroring Configuration
VLAN Configuration
Priority Configuration
MAC Address Configuration
Misc Configuration
Main Menu

Configure the sysytm, IP, and password.
Tab=Next Item  BackSpace=Previous Item  Enter=Select Item
```

(3) Select **IP Configuration** with Tab and press Enter

```
VDSL Switch :      Device Configuration
=====

Device Information
IP Configuration
Change Username
Change Password
Previous Menu

Configure the device information.
Tab=Next Item  BackSpace=Previous Item  Enter=Select Item
```

```
VDSL Switch :      IP Configuration
=====

IP Address   : 192.168.16.254
Subnet Mask  : 255.255.255.0
Gateway      : 192.168.16.1

actions->  <Edit>          <Save>          <Quit>
Configure the IP Information.
Tab=Next Item  BackSpace=Previous Item  CTRL+A=Action menu  Enter=Select Item
```

(4) Change IP sequence

- Select **Edit** item to Change IP address, Subnet Mask and Gateway
- Use **CTRL+A** key combination to return to actions menu
- Select **Save** to save change and go back to System Configuration page
- Select **Previous Menu** item to quit System Configuration page
- Select **Main Menu** item to quit IP DSLAM Configuration page and go back to Main Menu
- Select **Reboot IP DSLAM** menu item
- Select **Restart** menu item to reboot your IP DSLAM with new configuration.

3.2 Remote Network Management

3.2.1 IP Setting

You must first setup the "IP Address" with the local serial console port (RS-232 Port). Then you can use this IP address to control the VDSL IP DSLAM by Telnet and WEB. You could also change your computer's IP domain to be the same as that of the VDSL SWITCH. Then use the default IP address to control this VDSL IP DSLAM.

Default TCP/IP settings of the VDSL Switch

IP Address : 192.168.16.250

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.16.1

1. Remote control by "Telnet"

To enter Telnet, type the IP address of the IP DSLAM to connect with the management system, then type the username and password.

Default User Name: admin

Default Password: 123

Notes:

I. For security reasons, we limit the number of user login sessions on Telnet and Console port. You cannot login with Telnet and the serial Console port at the same time. You can login with Telnet and the Console port at different times. You should close the console port by logging out when leaving. Otherwise you will not be able to login by Telnet.

II. WEB Login does not limit user login sessions.

2. Remote control by "WEB"

3.2.2 Web Management Function

1. Use a Web browser (IE, Firefox, Netscape, etc.) to manage and monitor the switch. The default values are as follows: If you need change the IP address from its default value, you can use console mode to modify it. (see 3.1 In-band Management)

IP Address: 192.168.16.250

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.16.1

User Name: admin Password: 123

2. You can then browse to [http:// 192.168.16.250](http://192.168.16.250), and type in the user name and password as shown below.



Chapter 3 Management Configuration

3.2.2.1. Web Management Home Overview

This is the VDSL IP DSLAM's Home Page.



3.2.2.2. Port status

On this page you can see all current port statuses

1. **Config:** Display the state of user configuration.
2. **Actual:** Display the actual state of the connection.
3. **State:** Displays the port status; disable means unlink port, enable means link port.
4. **Link Status:** Down indicates "No Link", while UP indicates "Link".
5. **Auto Negotiation:** Displays the Switch auto negotiation mode.
6. **Speed status:** Ports 9 & 10 are 10/100/1000Mbps Ethernet and Ports 1-8 are 5/15/25Mbps VDSL.
7. **Duplex status:** Displays full-duplex or half-duplex mode.
8. **Flow control:** Displays flow control status enabled or disabled mode.

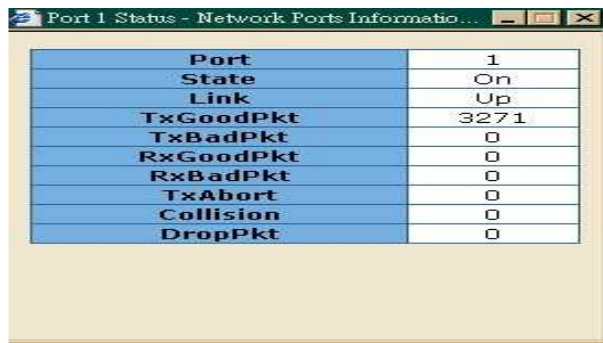
Port Status

The following information provides a view of the current status of the unit.

Port Num	State		Link Status	Auto Negotiation		Speed Status		Duplex Status		Flow Control	
	Config	Atual		Config	Atual	Config	Atual	Config	Atual	Config	Atual
1	On	Off	Down	Auto	Auto	Auto	15M	Full	Full	On	On
2	On	Off	Down	Auto	Auto	Auto	15M	Full	Full	On	On
3	On	Off	Down	Auto	Auto	Auto	15M	Full	Full	On	On
4	On	Off	Down	Auto	Auto	Auto	15M	Full	Full	On	On
5	On	On	Up	Auto	Auto	Auto	15M	Full	Full	On	On
6	On	On	Up	Auto	Auto	Auto	15M	Full	Full	On	On
7	On	Off	Down	Auto	Auto	Auto	15M	Full	Full	On	On
8	On	Off	Down	Auto	Auto	Auto	15M	Full	Full	On	On
T	On	Off	Down	Auto	Auto	Auto	100	Full	Full	On	On
E	On	On	Up	Auto	Auto	Auto	100	Full	Full	On	On

Chapter 3 Management Configuration

You must click on the actual physical port on the graphic image of the DSLAM to view the individual port status in detail. Then the user can see a single port counter as follows.



Port	1
State	On
Link	Up
TxGoodPkt	3271
TxBadPkt	0
RxGoodPkt	0
RxBadPkt	0
TxAbort	0
Collision	0
DropPkt	0

3.2.2.3. Port Statistics

The following information provides a view of the current Port Statistics of the unit.

Port Statistics

The following information provides a view of the current status of the unit.

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
1	On	Up	3299	0	0	0	0	0	0
2	On	Up	3297	0	0	0	0	0	0
3	On	Up	3297	0	0	0	0	0	0
4	On	Up	3295	0	0	0	0	0	0
5	On	Up	3295	0	0	0	0	0	0
6	On	Up	3296	0	0	0	0	0	0
7	On	Up	3295	0	0	0	0	0	0
8	On	Up	3295	0	0	0	0	0	0
T	On	Up	3296	0	0	0	0	0	0
E	On	Up	226866	0	213746	0	0	0	3695

3.2.2.4. Administrator

There are many management functions for configuration or display, including:

IP Address : sets the units IP address, subnet mask and gateway

Switch Setting : includes basic and advanced Layer 2 switch settings

Port Controls : adjusts the user configuration for each port's state, auto, speed, duplex and flow control

Link Aggregation : provides the ability to aggregate any or all ports into 1 to 4 groups

Filter Database : provides for static MAC, port security and MAC filtering functions

VLAN Config : if active, the VLAN configuration is done here

Spanning Tree : provides the ability to configure STP between any ports

Port Mirroring : configures the port mirroring function for traffic sniffers

SNMP : configures the SNMP MIB parameters, community strings and trap managers

SNR Status : displays the signal to noise ratio figures for all VDSL ports

Security Manager : changes the admin password

TFTP Update Firmware : set the Trivial FTP IP address and image name used for upgrading firmware

Configuration Backup : provides export and import ability of the internal configuration

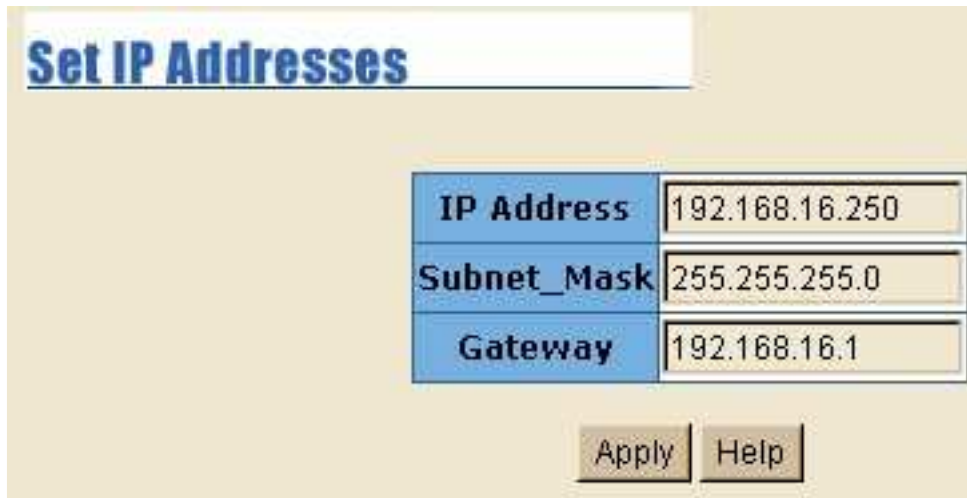
Reset System : returns the device to factory defaults

Reboot : does a soft reboot of the device and applies any configuration changes

Chapter 3 Management Configuration

3.2.2.5. IP Address

1. The administrator can configure the IP Settings by filling in new values, then clicking the apply button.
2. The new IP address is applied after a soft reset or power re-cycle is performed.



The screenshot shows a web-based configuration interface titled "Set IP Addresses". It contains three input fields for IP configuration: "IP Address" with the value "192.168.16.250", "Subnet_Mask" with the value "255.255.255.0", and "Gateway" with the value "192.168.16.1". Below these fields are two buttons: "Apply" and "Help".

IP Address	192.168.16.250
Subnet_Mask	255.255.255.0
Gateway	192.168.16.1

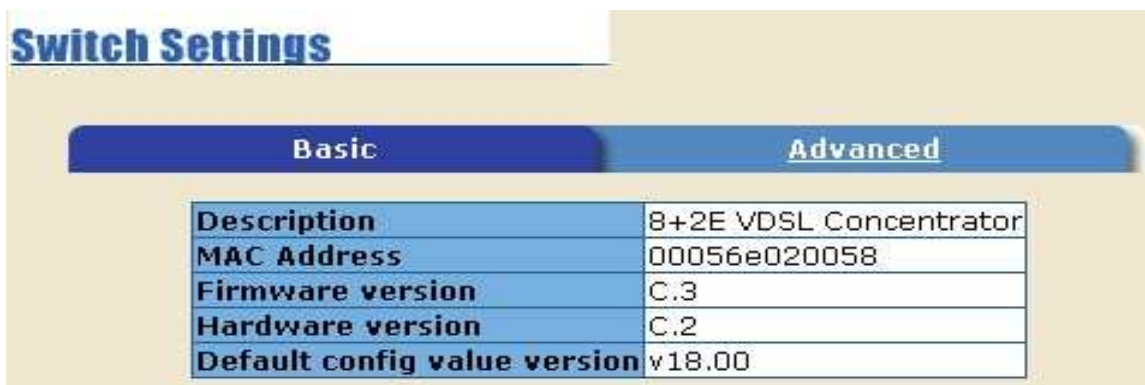
Apply Help

The Default IP is 192.168.16.250

3.2.2.6. Switch Settings

Basic

1. **Description** : Displays the device type name.
2. **MAC Address** : The unique Ethernet hardware address assigned by manufacturer
3. **Firmware Version** : Displays the switch's firmware version.
4. **Hardware Version** : Displays the switch's hardware version.
5. **Default config value version**: Displays the factory default EEPROM value version.

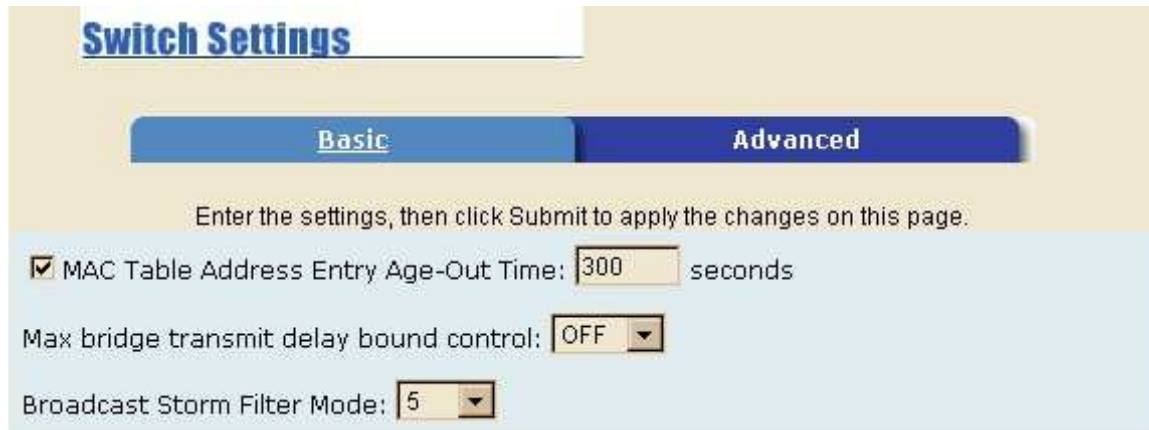


The screenshot shows a web-based configuration interface titled "Switch Settings". It has two tabs: "Basic" (selected) and "Advanced". Below the tabs is a table displaying various switch settings.

Switch Settings	
Description	8+2E VDSL Concentrator
MAC Address	00056e020058
Firmware version	C.3
Hardware version	C.2
Default config value version	v18.00

Advanced

1. **MAC Address Age-out Time** : The number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300~765 seconds. Default is 300 seconds.
2. **Max bridge transit delay bound control** : Limit the packets queuing time in the store and forward switch. If enabled, the packets queued exceeding the setting value will be dropped. The valid values are 1sec, 2 sec, 4 sec and off. Default is 4 seconds.
3. **Broadcast Storm Filter** : To configure broadcast storm control, enable it and set the upper threshold for each individual port. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold values are 5%, 10%, 15%, 20%, 25% and off. The default is 5%.



Switch Settings

Basic **Advanced**

Enter the settings, then click Submit to apply the changes on this page.

☒ MAC Table Address Entry Age-Out Time: seconds

Max bridge transmit delay bound control:

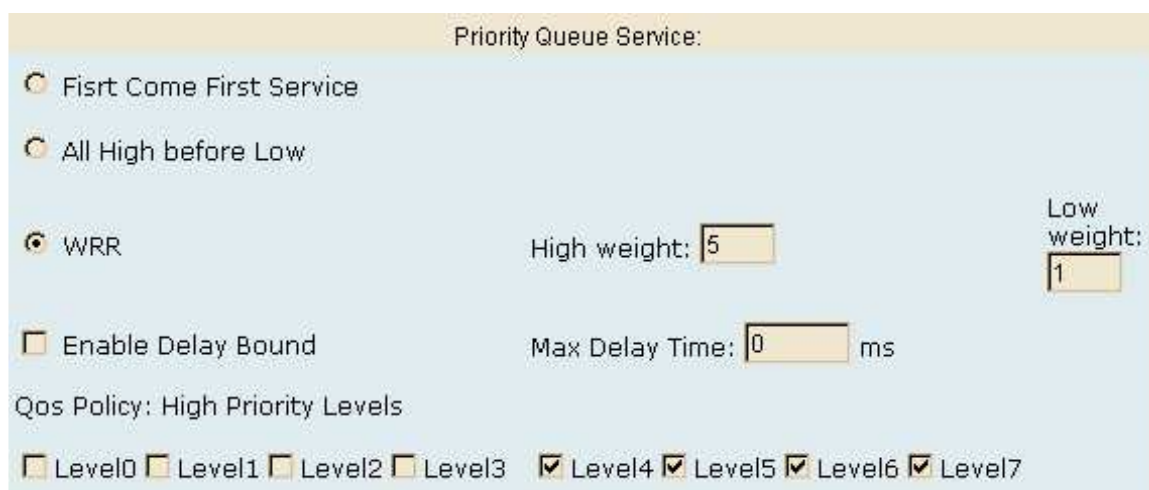
Broadcast Storm Filter Mode:

Priority Queue Service settings:

1. **First Come First Served** : The sequence of packets sent is dependant on the arrive order.
2. **All High before Low** : High priority packets are sent before low priority packets.
3. **Weighted Round Robin** : Select the preference given to packets in the switch's high-priority queue. This option represents the number of high priority packets sent before one low priority packet is sent. For example, 5 High : 2 Low means that the switch sends 5 high priority packets before sending 2 low priority packets.
4. **Enable Delay Bound** : Limits the low priority packets queuing time in the switch. The default Max Delay Time is 255ms. If the low priority packet stays in the switch exceeding Max Delay Time, it will be sent. The valid range is 1~255 ms.

NOTE: Make sure the "Enable Delay Bound" is checked before entering a "Max Delay Time" values. The Max Delay Time value works under the Enable Delay Bound control.

5. **QoS Policy** : High Priority Levels: 0~7 priority levels may be mapped to high or low queue.



Priority Queue Service:

☐ First Come First Service

☐ All High before Low

☒ WRR

High weight: Low weight:

☐ Enable Delay Bound

Max Delay Time: ms

Qos Policy: High Priority Levels

☐ Level0 ☐ Level1 ☐ Level2 ☐ Level3 ☒ Level4 ☒ Level5 ☒ Level6 ☒ Level7

Protocol Enable Setting:

1. **Enable Spanning Tree Protocol** : Default recommend to enable STP
2. **Enable IGMP** : enable Internet Group Multicast Protocol
3. **VLAN Protocol** : 802.1Q (Tagging Based) without GVRP VLAN mode
802.1Q (Tagging Based) with GVRP VLAN mode

Protocol Enable Setting

☒ Enable STP Protocol

☐ Enable IGMP Protocol

VLAN Operation Mode: No VLAN

☐ Assign management

Auto Speed SNR margin Value Setup: Maximum Minimum

GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol)

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, it will send a GVRP request using the VID of a VLAN defined on the switch, and the switch will automatically add that device to the existing VLAN.

Assign management IP address to specific VLAN

This can limit the management system for only a specific VLAN. This function must first enable 802.1Q.

Auto Speed SNR margin value setup: Maximum Minimum

VDSL Speed auto adaptive function is based on SNR value. You can specify target SNR margins.

Maximum: When SNR value is bigger than Maximum value, the VDSL speed will increase.

Minimum: When SNR value is smaller than Minimum value, the VDSL speed will decrease.

The priority of Minimum setup is higher than Maximum setup.

3.2.2.7. Console Port Information

The console is a standard UART interface which communicates with the Serial Port.

the user can use Windows® HyperTerminal™ program to link to the serial port. Configure with these parameter:

Bits per seconds: 9600

Data bits: 8

Parity: none

Stop Bits: 1

Flow control: none

3.2.2.8. Port Controls, VDSL Speed Control and port Enable/Disable

This section shows you how to change each port status and speed mode

State : You can disable or enable the VDSL port here

Auto Negotiation : You can set auto-negotiation enabled or disabled for the VDSL port here

Speed : You can change the VDSL Speed mode as 5Mbps, 15Mbps or 25Mbps

Speed Default Value : Auto

Distance range between VDSL & VDSL modem when standard 24 AWG (0.5mm) wire is used:

5 Mbps -> 1.7 Km (Without PBX)

15 Mbps -> 1.1 km (Without PBX)

25 Mbps -> 0.6 km (Without PBX)

Duplex : User can set full-duplex or half-duplex mode on the Ethernet port. The VDSL port is fixed at Full Duplex.

Flow Control : Full: User can set flow control function enabled or disabled in Full mode.

Half: User can set backpressure enabled or disabled in Half mode.

Change Speed procedures:

1. Confirm the phone cable has been connected between the IP DSLAM and the VDSL modem.
2. Power on the IP DSLAM and VDSL modem.
3. The IP DSLAM will start auto-speed negotiation reboot.

The IP DSLAM will try 25M mode to link with VDSL modem, if that fails the negotiation will try 15M mode to link with the VSL modem, and if this fails, the auto negotiation will drop to 5M and try to re-link with the VDSL modem. Please note that with any length of phone cable change, the VDSL modem must re-power and re-negotiate the speed again.

Please wait 5 ~ 120 seconds until the VDSL port link is up, depending on the length of phone cable.

Port	State	Auto Negotiation	Speed	Duplex	Flow Control
1	Enable	Enable	10	Full	Enable
2					
3					

Apply

*Note: The VDSL ports support auto-speed negotiation. The speed mode depends on phone cable length and crosstalk (noise) issues. Any re-negotiation of speed requires re-plugging the phone line and re-powering IP DSLAM or modem. The speed negotiation may take up to 2 minutes.

25M/25M symmetric runs at up to 600 meters

15M/15M symmetric runs at up to 1.1km

5M/5M symmetric runs at up to 1.7km

The above speed modes were tested based on 24 AWG twist pair phone cable without PBX connection. We do not recommend setting the speed unless necessary. Both VDSL IP DSLAM and modem must be set at the same speed in order to link successfully. Auto setting on both is the preferred method.

3.2.2.9. Link Aggregation

The Link Aggregation Control Protocol (LACP) is part of IEEE-802.3ad that allows bundling of several physical ports to form a logical channel. LACP allows a switch to automatically negotiate the bundle. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode. For more detailed information refer to IEEE 802.3ad standard document.

Aggregator setting

Trunking

Aggregator Setting Aggregator Information State Activity

System Priority: 1

Group ID: Group1 << Get

LACP: Disable

Work Ports: 0

<< Add << Remove >>

port1
port2
port3
port4
port5
port6
port7
port8

Apply Delete Help

Chapter 3 Management Configuration

1. **System Priority** : A value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID** : You may create a link aggregation across two or more ports, choose the "group id" and click "Get".
3. **LACP** : If enabled, the group is an LACP static trunking group. If disabled, the group is a local static trunking group. All ports support LACP dynamic trunk grouping. If connected to a device that also supports LACP, the LACP dynamic trunking group will be created automatically.
4. **Work ports** : The max number of ports that can be aggregated at the same time. If in LACP static trunking group, the excess ports will standby and be able to aggregate if the work ports fail. If in local static trunking group, the number must be the same as group ports.
5. Select the ports to join the trunking group
6. If LACP is enabled, you can configure LACP Active/Passive status for each port.
7. Click Apply.

Aggregator Information

When you are setting the LACP aggregator, you can see the relation information here.

This page show the Active and Partner trunking group 1 with port 1, 2, and 3.

Trunking

Aggregator Setting | **Aggregator information** | **State Activity**

The following information provides a view of LACP current status.

Static Trunking Group	
Group Key	1
Port_No	1 2 3

State Activity

Active (select): The port automatically sends LACP protocol packets.

Passive (no select): The port does not automatically sends LACP protocol packets, and responds only if it receives LACP protocol packets from another connected device.

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunking. A link which has two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for LACP protocol packets from the opposite device.
2. If you are activate LACP's state active, then when you are select the trunking port, the active status will be created automatically.

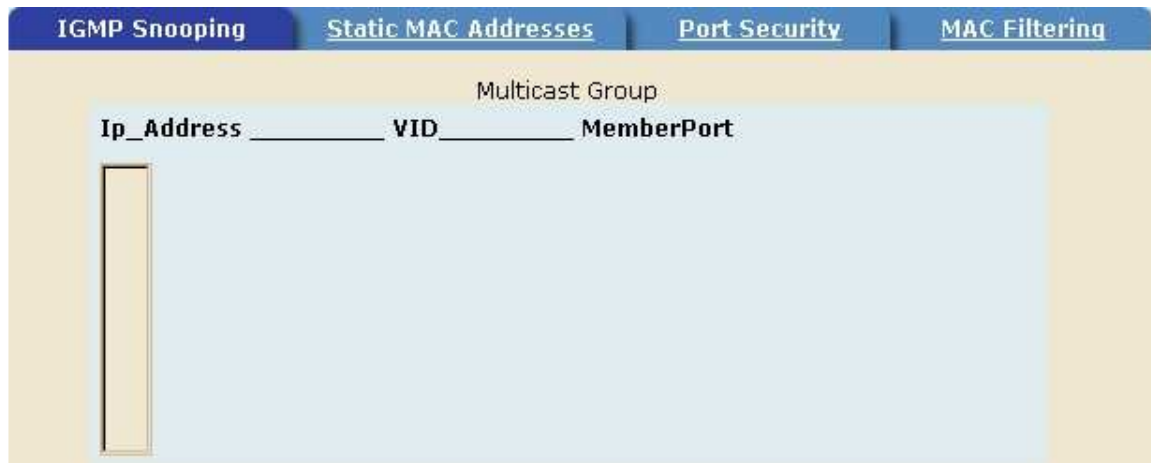
Trunking

Aggregator Setting | **Aggregator information** | **State Activity**

Port	LACP State Activity	Port	LACP State Activity
1	<input type="checkbox"/> Active	5	<input type="checkbox"/> Active
2	<input type="checkbox"/> Active	6	<input type="checkbox"/> Active
3	<input type="checkbox"/> Active	7	<input type="checkbox"/> Active
4	<input type="checkbox"/> Active	8	<input type="checkbox"/> Active

3.2.2.10. Filter Database

IGMP Snooping



The IP DSLAM supports IP multicasting. IGMP protocol can be enabled via the web management's switch setting advanced page, and then can display the IGMP snooping information on this same page. Different multicast groups may be viewed, along with VID and member port. The IP multicast addresses range is from 224.0.0.0 through 239.255.255.255.

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. For more information about IGMP, please refer to RFC988, 1054, 1112, 1812.

IGMP has three fundamental types of messages as follows:

Message	Description
Query	A message sent from the query agent (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the query agents to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the query agents to indicate that the host has quit to be a member of a specific multicast group.

Static MAC Address

Forwarding and Filtering

IGMP Snooping **Static MAC Addresses** Port Security MAC Filtering

Static addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address _____ PORT _____ VID _____

Mac Address

Port num

Vlan ID

When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when it is disconnected or powered-off and again becomes active on the network.

1. To add a static MAC address, from the main menu, click administrator, then click Filter Database.
2. Click Static MAC Addresses. In the MAC address box, enter the MAC address for the port which should permanently forward traffic, regardless of the device's network activity.
3. In the Port Number box, select a port number. If tag-based (IEEE 802.1Q) VLANs are setup on the switch, static addresses are associated with individual VLANs. Type the VID (VLAN ID) to associate it with the MAC address.
4. Click "add"

Port Security

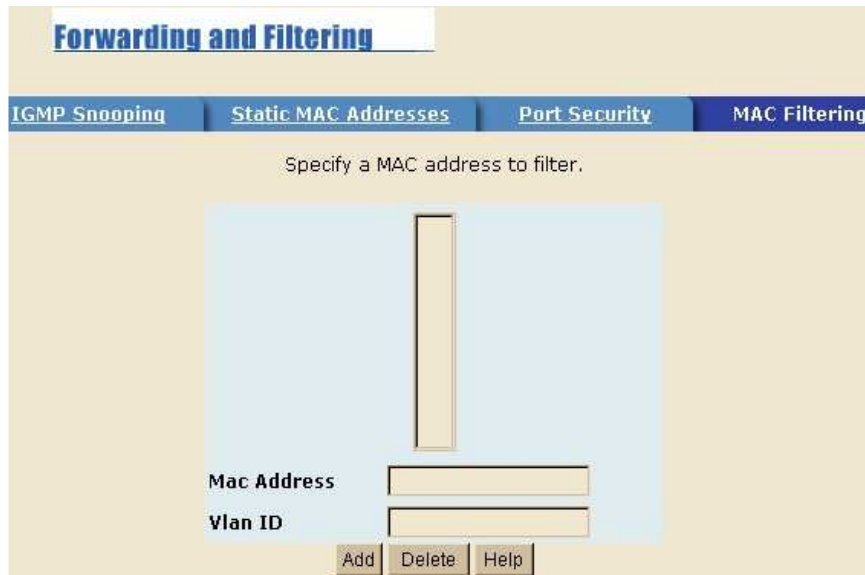
Forwarding and Filtering

IGMP Snooping Static MAC Addresses **Port Security** MAC Filtering

Port	Enable Security (disable for MAC Learning)	Port	Enable Security (disable for MAC Learning)
1	<input type="checkbox"/>	6	<input type="checkbox"/>
2	<input type="checkbox"/>	7	<input type="checkbox"/>
3	<input type="checkbox"/>	8	<input type="checkbox"/>
4	<input type="checkbox"/>	T	<input type="checkbox"/>
5	<input type="checkbox"/>	E	<input type="checkbox"/>

A port in security mode will be "locked" without permission for address learning. Only the incoming packets with MAC already existing in the address table can be forwarded normally. The administrator can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can be used on the secured port. Enter the settings, then click Submit to apply the changes on this page.

MAC Filtering



MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. For example, if your network is congested because of high utilization from one MAC address, you can filter all traffic transmitted from that MAC address, restoring network flow while you troubleshoot the problem.

3.2.2.11. VLAN configuration

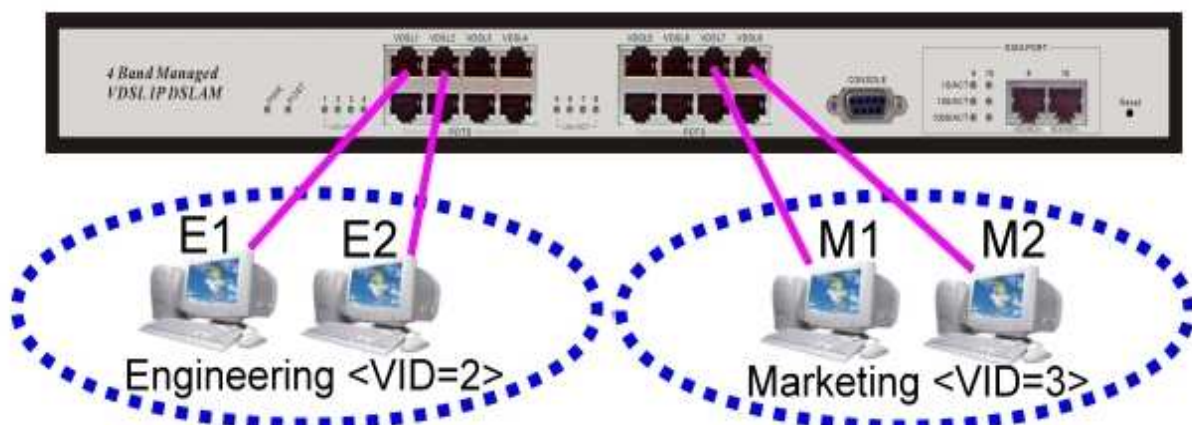
A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent to physically reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically. The IP DSLAM supports port-based and protocol-based VLAN in the web management page. In the default configuration, VLAN support is enabled and all ports on the switch belong to the default VLAN ID, VID 1.

Supports Multiple VLAN (IEEE 802.1Q VLAN)

Port-based Tagging rule VLAN is an IEEE 802.1Q specification standard. Using this standard, it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. The Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

Supports Protocol-based VLAN

In order for an end station to send packets to different VLAN, it has to be capable of either tagging packets it sends with VLAN tags or attaching to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default VID but also other information about the packet, such as the protocol. The IP DSLAM will support protocol-based VLAN classification by means of both built-in knowledge of layer 2 packet formats used by selected popular protocols, such as Novell IPX and AppleTalk's EtherTalk, and some degree of programmable protocol matching capability.



Basic

Tag-based (IEEE 802.1Q) VLAN

Basic Port VID

VLAN Information

default 1

Add Edit Delete PrePage NextPage Help

Create a VLAN and add tagged member ports to it.

1. From the main menu, click administrator -- VLAN configuration.
2. Click "Add"
3. Type a name for the new VLAN.
4. Type a VID (between 2-4094). The default is 1.
5. From the Available ports box, select ports to add to the switch and click Add.
6. Click "Apply".

Port VID

Tag-based (IEEE 802.1Q) VLAN

Basic Port VID

Assign a Port VLAN ID (1-4094) for untagged traffic on each port, then click Submit to apply the changes on this page.

NO	PVID	Ingress Filtering 1	Ingress Filtering 2	NO	PVID	Ingress Filtering 1	Ingress Filtering 2
1	1	Enable	Disable	6	1	Enable	Disable
2	1	Enable	Disable	7	1	Enable	Disable
3	1	Enable	Disable	8	1	Enable	Disable
4	1	Enable	Disable	T	1	Enable	Disable
5	1	Enable	Disable	E	1	Enable	Disable

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)

Ingress Filtering Rule 2
(Drop Untagged Frame)

Apply Default Help

Configure port VID settings

From the main Tag-based (IEEE 802.1Q) VLAN page, click Port VID Settings. Assign a port VLAN ID (1-4094) for untagged traffic on each port. Click "Submit" to apply changes.

Port VID (PVID)

Sets the Port VLAN ID that will be assigned to untagged traffic on a given port. For example, if port 10's Default PVID is 100, all untagged packets on port 10 will belong to VLAN 100. The default setting for all ports is VID 1. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. Only one untagged VLAN is allowed per port.

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN be forwarded if the port belongs to that VLAN. The IP DSLAM has two ingress filtering rules as follows:

Ingress Filtering Rule 1 : Forward only packets with VID matching this port's configured VID

Ingress Filtering Rule 2 : Drop Untagged Frames

3.2.2.12. Spanning Tree

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, it ensures that only one path at a time is active between any two nodes on the network. You can enable Spanning-Tree Protocol through the web management's switch setting advanced item, select enable Spanning-Tree protocol. We are recommended that you enable STP on all switches to ensure a single active path on the network.

1. You can view spanning tree information about the root bridge on the following screen:

Set Spanning Tree	
Root Bridge Information	
Priority	30000
Mac Address	00056ecccccc
Root_Path_Cost	10
Root Port	10
Max Age	20
Hello Time	2
Forward Delay	15

2. You can view the spanning tree status of the switch from the following screen.

STP Port Status			
PortNum	PathCost	Priority	PortState
1	10	128	FORWARDING
2	10	128	FORWARDING
3	10	128	FORWARDING
4	10	128	FORWARDING
5	10	128	FORWARDING
6	10	128	FORWARDING
7	10	128	FORWARDING
8	10	128	FORWARDING
T	10	128	FORWARDING
E	10	128	FORWARDING

3. You can set new values for STP parameters, then click set Apply button to modify.

Configure Spanning Tree Parameters	
Priority (1-65535)	<input type="text" value="32768"/>
Max Age (6-40)	<input type="text" value="15"/>
Hello Time (1-10)	<input type="text" value="3"/>
Forward_Delay_Time(4-30)	<input type="text" value="5"/>
<input type="button" value="Apply"/>	

Parameter	Description
Priority	You can change the priority value; A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. Enter a number 1 through 65535.
Max Age	You can change Max Age value; The number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration. Enter a number 6 through 40.
Hello Time	You can change Hello time value; The number of seconds between the transmission of Spanning-Tree Protocol configuration messages. Enter a number 1 through 10.
Forward Delay time	You can change forward delay time; The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening state to the forwarding state. Enter a number 4 through 30.

Chapter 3 Management Configuration

4. The following parameters can be configured on each port. Click Apply button to modify.

Configure Spanning Tree Port Parameters

Port Number	Priority (0 - 255; Default 128)	Path Cost (1 - 65535; Default 10)
1 2 3 4 5	128	10

Apply Help

Parameter	Description
Port Priority	You can make the port more or less likely to become the root port by setting the number lower or higher. The range is 0-255 and default setting is 128. The lowest number has the highest priority. If you change this value, you must reboot the switch.
Path Cost	Specifies the path cost of the port that the switch uses to determine which ports are the forwarding ports. The lowest numbers are the forwarding ports. The range is 1-65535 and default value is based on IEEE802.1D 10Mb/s = 50-600 100Mb/s = 10-60 1000Mb/s = 3-10. If you change this value, you must reboot the switch.

3.2.2.13. Port Mirroring

Port Mirroring is a method for allowing the monitoring of traffic in switched networks. Traffic through ports can be monitored by one specific port. In other words, traffic going in or out the monitored ports will be duplicated on the mirror port.

Running Analysis State : Enable or disable the port mirroring function.

Analysis Port : Analysis port can be used to see all monitor port traffic. You can connect mirrored port to LAN Analyzers, Session Wall or Wireshark Packet Capture.

Monitor Ports : The ports you want to monitor. All monitor port traffic will be copied to mirrored port. You can select a maximum of 9 monitor ports in the switch. If you want to disable the function, you must unselect all the monitor ports.

Monitor Rx : Monitored receive frames from the port.

Monitor Tx : Monitoring sent frames from the port.

Port Sniffer

Running Analysis State: DISABLE

Analysis Port: None

Monitor Ports	Monitor Rx	Monitor Tx
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
T	<input type="checkbox"/>	<input type="checkbox"/>
E	<input type="checkbox"/>	<input type="checkbox"/>

Apply Default Help

3.2.2.14. SNMP


Any Network Manager running the Simple Network Management Protocol (SNMP) can manage the switch, provided the Management Information Base (MIB) is installed correctly on the management station. SNMP is a Protocol that governs the transfer of information between manager and agent. The VDSL SWITCH support SNMP v1.

1. Use this page to define workstations as trap managers and to enter SNMP community strings. The administrator can also define name, location, and contact person for the switch. Fill in the system options data, and then click Apply to update the changes on this page.

Name: Enter a name to be used for the switch.

Location: Enter the location of the switch.

Contact: Enter the name of a person or organization.



The image shows a web form titled "SNMP Management" with a sub-section "System Options". It contains three text input fields labeled "Name:", "Location:", and "Contact:". Below these fields are two buttons: "Apply" and "Help".

2. Community strings serve as passwords and can be entered as one of the following:



The image shows a web form titled "Community Strings". It has two main sections: "Current Strings:" and "New Community String:". The "Current Strings:" section contains a list box with "public_RO" and buttons for "<< Add <<" and "Remove". The "New Community String:" section contains a text input field labeled "String:" and two radio buttons labeled "RO" (selected) and "RW".

Read only: Enables requests accompanied by this string to display MIB-object information.

Read write: Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

3. Trap Manager



The image shows a web form titled "Trap Managers". It has two main sections: "Current Managers:" and "New Manager:". The "Current Managers:" section contains a list box with "(none)" and buttons for "<< Add <<" and "Remove". The "New Manager:" section contains two text input fields labeled "IP Address:" and "Community:".

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string.

Enterprise MIB contains two traps:

When IP DSLAM internal temperature is greater than 70°C, the system will send a "Temperature alarm " trap.

When the IP DSLAM's internal cooling FAN doesn't run, the system will send a "FAN speed alarm" trap.

3.2.2.15. SNR

The following information provides a view of the current VDSL Attenuation value of the unit for each port.
SNR(Signal to Noise Ratio)

SNR Status

The following information provides a view of the current VDSL Attenuation value of the unit.

SNR (Signal to Noise Ratio)

Port Num	SNR	
	Value	unit
1	42	db
2	No Link	db
3	No Link	db
4	No Link	db
5	No Link	db
6	No Link	db
7	No Link	db
8	No Link	db

3.2.2.16. Security Manager

1. Using this page, the administrator can change web management user name and password.

User name: Admin

Password: 123

Security Manager

User Name:	<input type="text" value="admin"/>
Assign/Change password:	<input type="password" value="***"/>
Reconfirm password:	<input type="password" value="***"/>
	<input type="button" value="Apply"/>

3.2.2.17. TFTP Update Firmware

1. The following menu options provide some system control functions to allow an administrator to update firmware and remote boot the switch system.

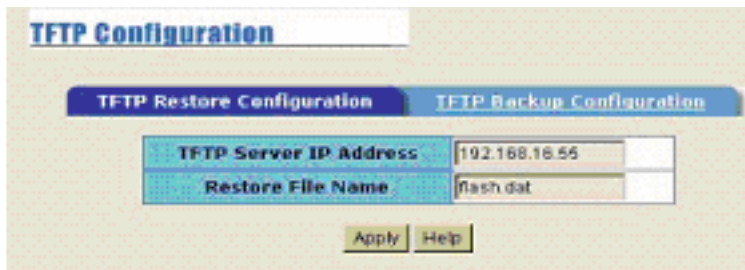
1. Start the TFTP server application.
2. Copy firmware update version image.bin to TFTP server's directory.
3. In the web management, select administrator - TFTP update firmware.
4. Keyin the TFTP server's IP address and the image filename.
5. Download new image.bin file in web management by pressing <update firmware>.



The screenshot shows a web page titled "TFTP Download New Image". It contains two input fields: "TFTP Server IP Address" with the value "192.168.16.55" and "Firmware File Name" with the value "image.bin". Below these fields are two buttons: "Apply" and "Help".

3.2.2.18. Configuration Backup/Restore

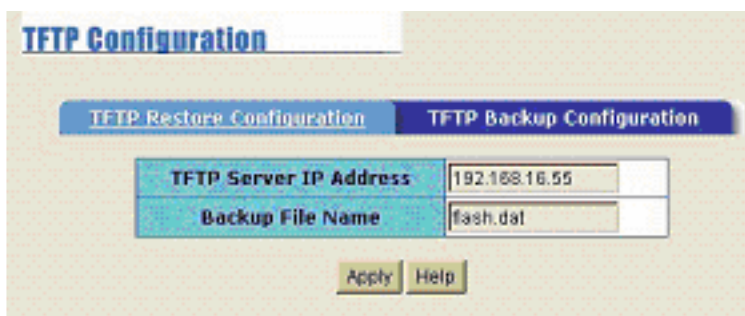
TFTP Restore Configuration



The screenshot shows a web page titled "TFTP Configuration" with two tabs: "TFTP Restore Configuration" (selected) and "TFTP Backup Configuration". Under the "TFTP Restore Configuration" tab, there are two input fields: "TFTP Server IP Address" with the value "192.168.16.55" and "Restore File Name" with the value "flash.dat". Below these fields are two buttons: "Apply" and "Help".

Use this page to set the TFTP server's IP address and restore filename. You can restore configuration values from here, but you first must have a backup file in the TFTP server. Press "Apply" and the switch will download backup configuration.

TFTP Backup Configuration



The screenshot shows a web page titled "TFTP Configuration" with two tabs: "TFTP Restore Configuration" and "TFTP Backup Configuration" (selected). Under the "TFTP Backup Configuration" tab, there are two input fields: "TFTP Server IP Address" with the value "192.168.16.55" and "Backup File Name" with the value "flash.dat". Below these fields are two buttons: "Apply" and "Help".

Use this page to set the TFTP server's IP address and name to give the configuration backup file. You can save current configuration values from here. Then go to the TFTP restore configuration page to restore the configuration values.

3.2.2.19. Reset System

Resets the IP DSLAM to factory default configuration.

Note. Please make sure the IP DSLAM has been disconnected from VDSL Modem.

3.2.2.20. Reboot

Reboot the IP DSLAM using software reset.

This page left blank intentionally.

4. Applications

VDSL may be used to provide a network architecture. Transforming an apartment into a Multiple-Family Home network area, sharing a single internet account for multiple users via Router & Cable Modem, the VDSL IP DSLAM can provide unlimited access time in the Internet at a reasonably low price.

Bridging Functions

The IP DSLAM provides full transparent bridging function. It automatically connects node addresses, that are later used to filter and forward all traffic based on the destination address. When traffic passes between devices attached to the shared collision domain, those packets are filtered from the IP DSLAM. But when traffic must be passed between unique segments (i.e., different ports of the IP DSLAM), a temporary link is set up between the IP DSLAM's port in order to pass this traffic, via the high-speed VDSL fabric.

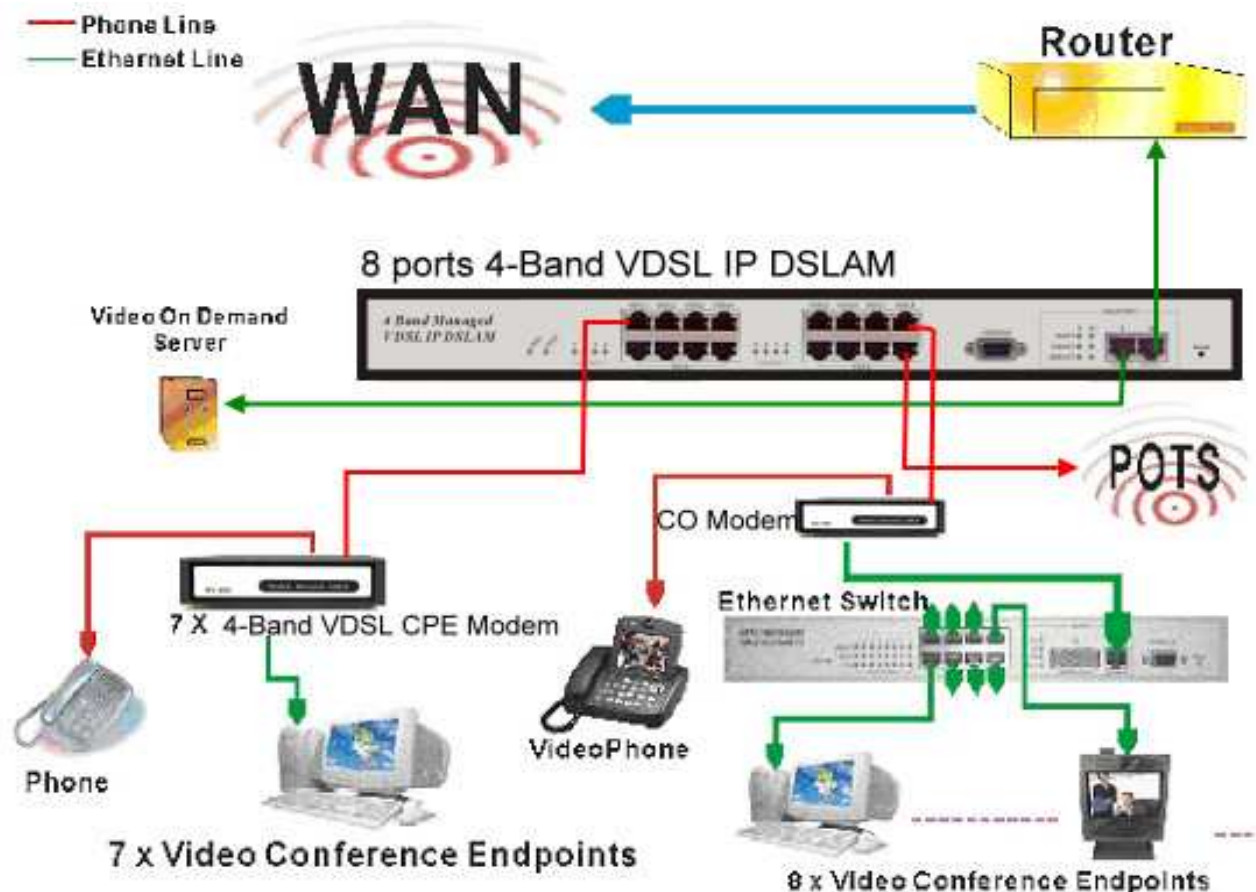
Transceiver function

The IP DSLAM supports Ethernet to VDSL conversion. It can transmit or receive packet from Ethernet port to the VDSL ports, or VDSL ports to Ethernet port.

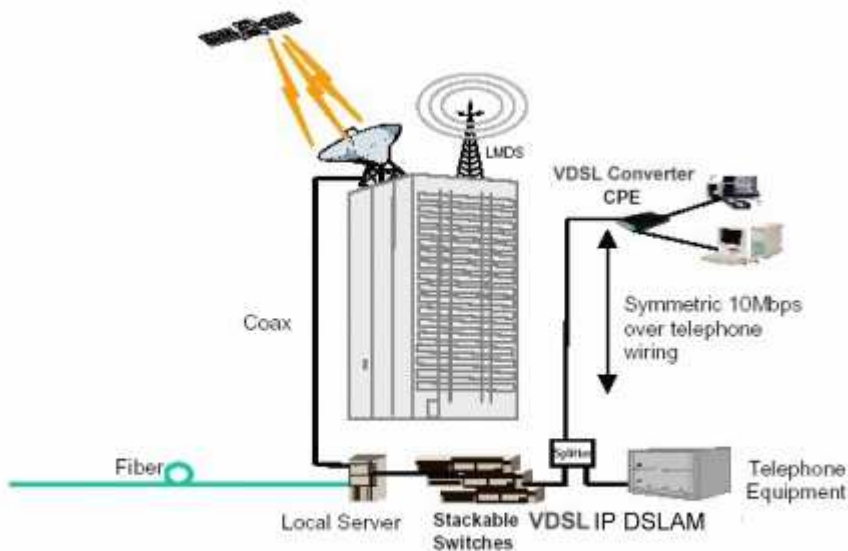
Flexible Configuration

The IP DSLAM is not only designed to segment your network, but also to provide a wide range of options in the configuration of home network connections. It can be used as a simple stand-alone IP DSLAM; or can be connected with another IP DSLAM, Cable modem, Router, xDSL, ISDN, gateway or other network interconnection devices in various configurations. Some of the common applications of the IP DSLAM are described in this chapter.

*Application for Video on demand and Video conference



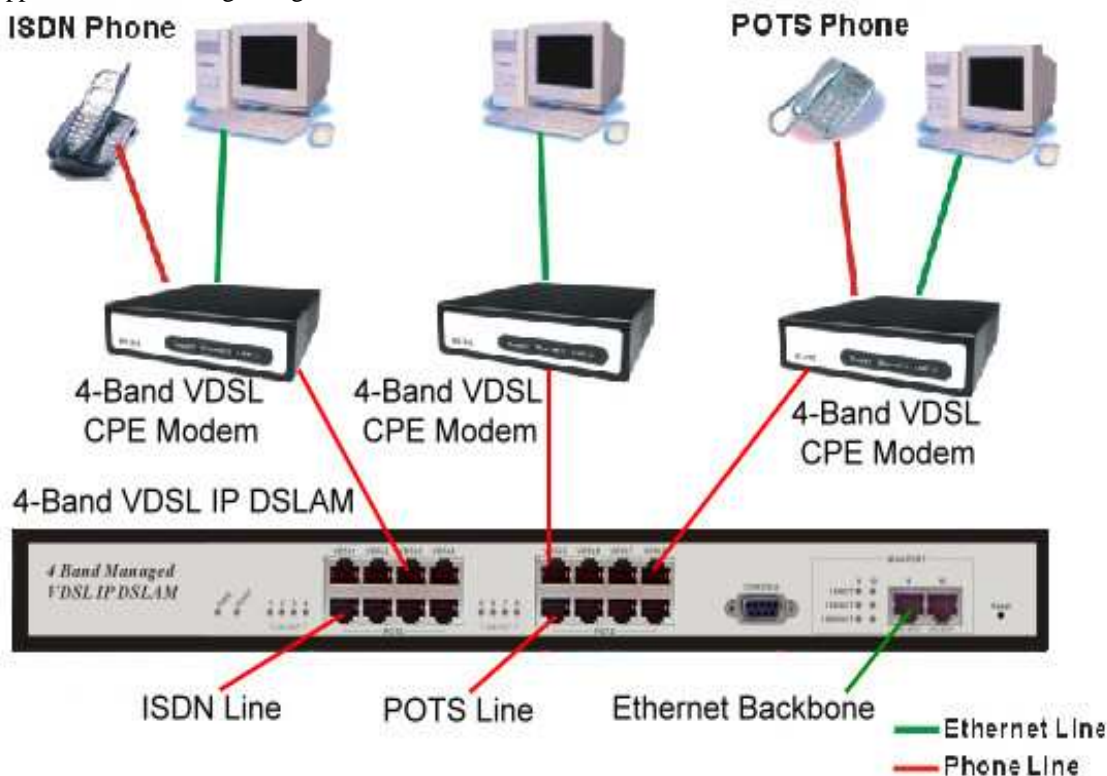
*Used in apartment complex for Internet access



Broadband Access Applications Utilizing VDSL IP DSLAM

The IP DSLAM provides a high speed, auto-speed transmission over existing telephone wiring. Using a single Internet account, the IP DSLAM can provide simultaneous independent Internet access to multiple users. Whether over ISDN Telephone system or POTS Telephone system, VDSL Technology will let you use the telephone system and VDSL network system at the same time.

* Application for sharing a single internet account



If multiple users would like to share a single internet account using the IP DSLAM, they should be connected to an IP sharing device, then to xDSL or Cable Modem.

Note: For network applications that actually require Router (e.g., Interconnecting dissimilar network types), attaching the IP DSLAM directly to a router can significantly improve overall networking performance.

High bandwidth backbone ready

The IP DSLAM provides 10/100/1000Mbps auto sensing for external trunk device (Fiber media converter, Wireless Bridge, xDSL & other WAN services)

Appendix A: Troubleshooting

Diagnosing VDSL Indicators

The VDSL IP DSLAM can be easily monitored through its comprehensive panel indicators. These indicators assist the network manager in identifying problems the IP DSLAM may encounter. This section describes common problems you may encounter and possible solutions.

Symptom: POWER indicator does not light up (green) after power on.

Cause: Defective power outlet, power cord, internal power supply

Solution: Check the power outlet by trying another outlet that is functioning properly. Check the power cord with another device. If these measures fail to resolve the problem, have the unit power supply replaced by a qualified distributor.

Symptom: Link indicator does not light up (green) after making a connection.

Cause: Network interface (e.g., a network adapter card on the attached device), network cable, or switch port is defective.

Solution: Verify that the switch and attached device are powered on.

Be sure the cable is plugged into both the switch and corresponding device.

Verify that the proper cable type is used and its length does not exceed specified limits.

Check the adapter on the attached device and cable connections for possible defects.

Replace the defective adapter or cable if necessary.

Symptom: VDSL always links at 5M/5M speed mode even with short phone cable.

Cause: VDSL auto speed lock up.

Solution: Please re-power the VDSL IP DSLAM.

Note : The VDSL IP DSLAM will also renegotiate auto speed function when the remote VDSL modem is re-powered on.

System Diagnostics

Power and Cooling Problems

If the POWER indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply as explained in the previous section. However, if the unit should turn itself off after running for a while, check for loose power connections, power loss or surges at the power outlet, and verify that the fan on back of the unit is unobstructed and running prior to shutdown. If you still cannot isolate the problem, then the internal power supply may be defective. In this case, contact your supplier for assistance.

Installation

Verify that all system components have been properly installed. If one or more components appear to be malfunctioning (e.g., the power cord or network cabling), test them in an alternate environment, where you are sure that all the other components are functioning properly.

Transmission Mode

The selections of the transmission mode for the Ethernet RJ-45 ports are auto-negotiated using the default method. Therefore, if the Link signal is disrupted (e.g., by unplugging the network cable and plugging it back in again, or by resetting the power), the port will try to reestablish communications with the attached device via auto-negotiation. If auto-negotiation fails, then communications are set to half duplex by default. Based on this type of industry-standard connection policy, if you are using a full-duplex device that does not support auto-negotiation, communications can be easily lost (i.e., reset to the wrong mode) whenever the attached device is reset or experiences a power fluctuation. The best way to resolve this problem is to upgrade these devices to versions that will support auto-negotiation.

Cabling

Verify that the cable type is correct. Be sure RJ-45 cable connectors are securely seated in the required ports. Use 100Ω straight-through cables for all standard connections. Use Category 5 cable for 100Mbps Fast Ethernet connections, or Category 3, 4 or 5 cables for standard 10Mbps Ethernet connections. Be sure RJ-45 phone wiring uses 18~26 AWG wire. Make sure all devices are connected to the network. Equipment any have been unintentionally disconnected from the network. When cascading two devices using RJ-45 station ports at both ends of the cable (i.e., not an MDI port), make sure a crossover cable is used. Crossover cable should only be used if an auto-MDIX port is not available.

Physical Configuration

If problems occur after altering the network configuration, restore the original connections, and try to track the problem down by implementing the new changes, one step at a time. Ensure that cable distances and other physical aspects of the installation do not exceed recommendations.

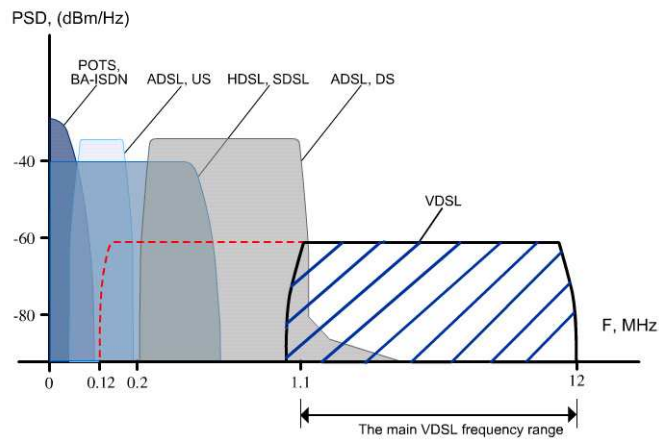
System Integrity

As a last resort, verify the switch integrity with a power-on reset. Turn the power to the switch off and then on several times. If the problem still persists, and you have completed all the preceding diagnostics, contact your dealer for assistance.

Appendix B: VDSL Spectrum



VDSL Technology – Requirements & Definitions Spectral Allocation



- Co-exists with legacy Voice and ISDN services
- Co-exists with other xDSL technologies
- Programmable notch filter to avoid Radio Frequency Interference

Slide 5

© 2002 Infineon Technologies COM/AC

All rights reserved

VDSL Spectral Allocation

Appendix C: Example of VLAN Setting

1. Port Based VLAN Setting

Web management → Administrator → Switch settings → Advanced:

Protocol Enable Setting→ VLAN Operation Mode: Select "Port_Based"

WRR

High weight:

weight:

☐ Enable Delay Bound

Max Delay Time: ms

QoS Policy: High Priority Levels

☐ Level0

☐ Level1

☐ Level2

☐ Level3

☒ Level4

☒ Level5

☒ Level6

☒ Level7

Protocol Enable Setting:

☒ Enable STP Protocol

☒ Enable IGMP Protocol

VLAN Operation Mode:

Apply

Default

Help

Web management → Administrator → Switch settings → Vlan Configuration:

VLAN Configuration

Port_based VLAN Information					

Add Edit Delete PrePage NextPage Help

Add VLAN Group 1, member: port 1 and port 9

VLANs

File Edit Help

VLAN Name: 1

Grp ID: 1

2
3
4
5
6
7
8
10

1
9

Add >>

<< Remove

Apply Help

2. Tag Based (IEEE 802.1Q) VLAN Setting

Web management → Administrator → Switch settings → Advanced:

Protocol Enable Setting → VLAN Operation Mode: Select "802.1Q without GVRP"

Protocol Enable Setting

☒ Enable STP Protocol
☐ Enable IGMP Protocol
 VLAN Operation Mode: 802.1Q without GVRP

Apply
Default
Help

Administrator → VLAN Configuration: Select "Port VID" in this stage, you can define each port's PVID and set traffic rules for each port.

Note: There are two basic rules for setting traffic filtering rule while you use Tag VLAN.

1. Ingress rule will take effect when the packet is "incoming".
2. Ingress rule 1 and 2 will be checked when you use tag. Otherwise the ingress rule will be meaningless.

Tag-based (IEEE 802.1Q) VLAN

Basic
Port VID

Assign a Port VLAN ID (1~4094) for untagged traffic on each port, then click Submit to apply the changes on this page.

No.	PVID	Ingress Filtering 1	Ingress Filtering 2	No.	PVID	Ingress Filtering 1	Ingress Filtering 2
1	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼	6	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼
2	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼	7	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼
3	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼	8	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼
4	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼	T	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼
5	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼	E	<input style="width: 50px;" type="text" value="1"/>	Enable ▼	Disable ▼

Ingress Filtering Rule 1
(Forward only packets with VID matching this port's configured VID)

Ingress Filtering Rule 2
(Drop Untagged Frame)

Apply
Default
Help

VLAN Configuration: Select "Basic"
Default_1 exists when you use 802.1Q Tag VLAN.
Highlight default_1 and click Edit button to add/remove each port.

Tag-based (IEEE 802.1Q) VLAN

Basic

Port VID

802.1Q with\without GVRP VLAN Information

default_1

Add

Edit

Delete

PrePage

NextPage

Help

In default_1 group, add in or remove group members.
Click Next button to set Tag or Untag for each assigned port.

Tag-based (IEEE 802.1Q) VLAN

Basic

Port VID

VLAN Name: default

VID: 1

Protocol Vlan: NONE

7
8
T
E

Add >>

<< Remove

1
2
3
4
5
6

Next

Help

From this page, you can set Tag or Untag for assigned port and click Apply button.

Tag-based (IEEE 802.1Q) VLAN

VLAN Name: default	
VLAN ID: 1	
Port_NO	Setting
1	Untag
2	Untag
3	Untag
4	Untag
5	Tag

Apply

Add in new group.

Click Add button into new group setting page.

Tag-based (IEEE 802.1Q) VLAN

Basic

Port VID

802.1Q with\without GVRP VLAN Information

default__1

Add Edit Delete PrePage NextPage Help

Add in new group page.
Fill in new group name into VLAN Name.
Set the VID number.
Add in new group members.
Click Next button.

Tag-based (IEEE 802.1Q) VLAN

Basic

Port VID

VLAN Name: Sample

VID: 2

Protocol Vlan: NONE

3
4
5
6
7
8

Add >>

<< Remove

1
2
T
E

Next

Help

Set Tag or Untag for group members and click Apply button.

Tag-based (IEEE 802.1Q) VLAN

VLAN Name: Sample

VLAN ID: 2

Port_NO	Setting	Port_NO	Setting
1	Untag	6	N/A
2	Untag	7	N/A
3	N/A	8	N/A
4	N/A	T	Untag
5	N/A	E	Tag

Apply

New group has been created, now you can highlight each group and click Edit or Delete button to modify or delete VLAN Group.

Tag-based (IEEE 802.1Q) VLAN

The screenshot displays a configuration window for '802.1Q with\without GVRP VLAN Information'. At the top, there are two tabs: 'Basic' (selected) and 'Port VID'. Below the tabs is a list box containing two entries: 'default' with a value of '1', and 'Sample' with a value of '2'. The 'Sample' entry is currently selected. At the bottom of the window, there is a row of six buttons: 'Add', 'Edit', 'Delete', 'PrePage', 'NextPage', and 'Help'.

802.1Q with\without GVRP VLAN Information	
default	1
Sample	2

Buttons: Add, Edit, Delete, PrePage, NextPage, Help



Transmission Units

**Far Eastern Vienna Technology Center
(Neihu Technology Park)
8F, No. 60 Zhouzi St.,
Neihu District,
Taipei, Taiwan
Phone: (886) 2-2659-1021
FAX: (886) 2-2799-1355
E-mail: info@ctcu.com
URL: <http://www.ctcu.com>**